UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MEGAN SCHWARZ, CAMILLE BURGAN, AND EUGENE BURGAN, individually and on behalf of all others similarly situated, Plaintiffs, v. PROGRESS SOFTWARE CORPORATION and PENSION BENEFIT INFORMATION, LLC d/b/a PBI RESEARCH SERVICES, Defendants.	Case No. **CLASS ACTION COMPLAINT** Jury Trial Demanded

Plaintiffs Megan Schwarz, Camille Burgan, and Eugene Burgan (together, "Plaintiffs"), individually and on behalf of all others similarly situated, by and through their undersigned counsel, bring this class action complaint against Progress Software Corporation ("PSC") and Pension Benefit Information, LLC d/b/a PBI Research Services ("PBI") (collectively, "Defendants"). Plaintiffs allege the following upon information and belief based on the investigation of counsel, except as to those allegations that specifically pertain to Plaintiffs, which are alleged upon personal knowledge.

INTRODUCTION

1. Plaintiffs bring this class action lawsuit on behalf of all persons who entrusted Defendants with sensitive personal information that was exposed in a data breach when, between May 29, 2023 and May 30, 2023, an unauthorized third party accessed PBI's internal MOVEit Transfer servers which contained individuals' sensitive personally identifying information ("PII") (the "Data Breach" or the "Breach").

2. PSC is a software company that offers software products and services to corporate and governmental entities, including cloud hosting and secure file transfer services such as MOVEit.

3. PBI processes information about employees or individuals for insurers engaged by employers, or for companies acting on such insurers' behalf, in connection with certain employee benefit programs. PBI uses PSC's MOVEit file transfer services.

4. Plaintiffs' claims arise from Defendants' failure to safeguard Plaintiffs' and Class members' PII. Plaintiffs' and Class members' PII was compromised due to Defendants' negligent and/or careless acts and the failure to protect their PII.

5. Employees provide the PII of their past and current employees and customers to PBI in connection with the services offered by PBI to its clients.

6. In carrying out its services, PBI utilizes MOVEit, the file sharing application created and operated by PSC, to securely transmit files containing sensitive consumer information. On or about May 31, 2023, PBI received a notification from PSC that an unauthorized external party had exploited a vulnerability within the MOVEit software. PBI then initiated an inquiry and determined that the unauthorized party had gained entry to one of PBI's MOVEit Transfer servers on May 29, 2023 and May 30, 2023. During this time, the unauthorized party acquired data containing sensitive PII held by PBI.

7. The hackers responsible for the Data Breach were subsequently identified as the Russian cyber gang, Clop.[1]

[1] Onur Demirkol, *US Government Under Siege: MOVEit Breach Exposes Critical Data to Ruthless Clop Ransomware Attack*, DATA CONOMY (June 19, 2023), available at https://dataconomy.com/2023/06/19/moveit-breach-data-clop-ransomware/ (last visited September 11, 2023).

8. Plaintiffs and members of the Class furnished sensitive and private PII directly or indirectly to PBI including their names, Social Security numbers, and birthdates

9. Defendants failed to properly secure and safeguard Plaintiffs' and the Class's PII that was stored within the MOVEit servers.

10. Despite purporting to act as a safe container for sensitive information, Defendants failed to take precautions designed to keep that information secure.

11. The data that PBI exposed was highly sensitive, including names, dates of birth, and Social Security numbers. The compromised data also allows individuals to infer that consumers were employed in certain sectors or use certain services offered by PBI.

12. The Data Breach affecting PSC's MOVEit file transfer tool impacted more than 15 million consumers in the United States.[2]

13. The sensitive nature of the data exposed through the Data Breach, including Social Security numbers, substantiates that Plaintiffs and Class members have suffered irreparable harm. Plaintiffs and Class members have lost the ability to control their private information and are subject to an increased risk of identity theft.

14. Defendants owed and owe a duty to Plaintiffs and Class members to maintain adequate security measures to safeguard the PII with which they were entrusted with. Defendants breached their duty by failing to implement and/or maintain adequate security practices.

15. PBI delayed acknowledging and giving notice of the Data Breach. PBI did not notify its customers of the Data Breach until mid-July 2023 (the "Notice Letter"). *See e.g.,*

[2] *See* Carly Page, *Millions affected by MOVEit mass-hacks as list of casualties continues to grow*, TECHCRUNCH https://techcrunch.com/2023/06/29/millions-affected-moveit-mass-hacks/ (last visited September 11, 2023).

Plaintiff Schwarz's Notice Letter, attached hereto as Exhibit A Notice Letter. PBI waited despite knowing that hackers accessed its account holders and customers information, and that sensitive PII was compromised.

16. As a result of PBI's inadequate digital security and notice process, Plaintiffs' and Class members' PII was exposed to criminals. Plaintiffs and the Class have suffered and will continue to suffer injuries including: financial losses caused by misuse of PII; the loss or diminished value of their PII as a result of the Data Breach; lost time associated with detecting and preventing identity theft; and theft of personal, medical, and financial information.

17. Plaintiffs brings this action individually and on behalf of a Nationwide Class of similarly situated individuals against Defendants for: negligence; negligence per se; breach of implied contract; and unjust enrichment.

JURISDICTION AND VENUE

18. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. At least one member of the Class defined below is a citizen of a different state than Defendants, and there are more than 100 putative Class members.

19. This Court has personal jurisdiction over Defendants because they both conduct substantial business in this jurisdiction. Further, this Court has general jurisdiction over Defendant PSC because its corporate headquarters is located in this District.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District, Defendant PSC is based in this District, Defendant PSC interacted with Defendant PBI in this District,

Defendant PSC designed, marketed, sold, and maintained the MOVEit transfer application in this District, and the harm caused to Plaintiffs and Class Members emanated from this District.

PARTIES

21. Plaintiff Megan Schwarz is a citizen of the state of New York. Plaintiff Schwarz received the Notice Letter dated July 14, 2023, notifying her that her information was part of the Data Breach. Plaintiff Schwarz has and will spend considerable time and effort monitoring her accounts to protect herself from identity theft. Plaintiff Schwarz fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach.

22. Plaintiff Camille Burgan is a citizen of the state of California. Plaintiff Camille Burgan received the Notice Letter dated July 21, 2023, notifying her that her information was part of the Data Breach. Plaintiff Camille Burgan has and will spend considerable time and effort monitoring her accounts to protect herself from identity theft. Plaintiff Camille Burgan fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach.

23. Plaintiff Eugene Burgan is a citizen of the state of California. Plaintiff Eugene Burgan received the Notice Letter dated July 21, 2023, notifying him that his information was part of the Data Breach. Plaintiff Eugene Burgan has and will spend considerable time and effort monitoring his accounts to protect himself from identity theft. Plaintiff Eugene Burgan fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach.

24. Defendant Progress Software Corporation is a corporation organized under the laws of the State of Delaware with its principal place of business located at 15 Wayside Road, Suite 4, Burlington, Massachusetts 01803.

25. Defendant Pension Benefit Information, LLC is a Delaware limited liability corporation with its principal place of business located at 333 S. 7th Street, Suite 2400, Minneapolis, Minnesota 55402.

FACTUAL BACKGROUND

The Data Breach

26. On or about May 31, 2023, PSC, the creator of the MOVEit software, Progress Software, announced on its Progress Community website that it was subject to a Data Breach[3] which compromised highly sensitive personal information of those that utilize the MOVEit software including names, dates of birth, and Social Security numbers.

27. PBI employs the MOVEit software, which is supplied by PSC. MOVEit's intended use is to safely move files as part of their routine operations. Within this process, PBI uploads, retains, shifts, or retrieves PII owned or held by various companies on whose behalf it provides its various services. This data is shared with PBI and managed using the MOVEit software.

28. On or about May 31, 2023, PSC informed PBI of a vulnerability in the MOVEit software that was exploited by an unauthorized third party.

[3] MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362), Progress Community, https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023 (last accessed September 12, 2023).

29. PBI reportedly performed an internal investigation into the scope of the vulnerability in MOVEit's software and the impact on its systems.[4] PBI's investigation revealed that the third party accessed one of its MOVEit servers between May 29, 2023 and May 30, 2023 and subsequently downloaded data from its servers.[5] On June 16, 2023, PBI completed a manual review of its records, and confirmed the identities of individuals affected by the Data Breach.

30. Individuals impacted by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

31. Plaintiffs and Class members are or were PBI customers or account holders that entrusted PBI with their PII.

PBI's Obligation and Responsibility to Protect Plaintiffs and Class members' PII

32. PBI provides audit and address research services for insurance companies, pension funds, and other organizations.[6]

33. PBI's Privacy Policy highlights its protection of PII, stating that:

> PBI recognizes the importance of protecting personal information. We use a variety of administrative, physical and technical security measures intended to safeguard your personal information.[7]

34. PBI further notes the "PBI Advantages" on its website, stating that consumers should have "Confidence Your Data is Secure," explaining that:

---

[4] *See* Exhibit A.
[5] *Id.*
[6] *See About PBI Research Services,* PBI https://www.pbinfo.com/who-we-are/ (last visited September 11, 2023).
[7] *See Privacy Policy,* PBI *https://www.pbinfo.com/privacy-policy/* (last visited September 11, 2023).

> Protecting and securing your information is our highest priority. Our formalized security program follows industry-recognized security frameworks and undergoes an annual SSAE 18 SOC 2, Type II audit.[8]

35. As a pension management business that handles consumers' personal information, PBI is legally required to protect personal information from unauthorized disclosure.

PBI's Failure to Prevent, Identify and Timely Report the Data Breach

36. PBI failed to take adequate measures to protect its computer systems and internal network against unauthorized access.

37. PBI also failed to properly select its information security partners that it relied upon to keep the personal information it held safe and secure.

38. PBI was not only aware of the importance of protecting the PII that it maintains, but it also touted its capability to do so. The PII that was exposed in the Data Breach is the type of private information that PBI knew or should have known would be the target of cyberattacks.

39. Despite its own knowledge and supposed expertise on the subject of cybersecurity, and notwithstanding the FTC's data security principles and practices,[9] PBI failed to disclose that its systems and security practices were inadequate to reasonably safeguard sensitive personal information.

40. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate

---

[8] *See About PBI Research Services,* PBI https://www.pbinfo.com/who-we-are/ (last visited September 11, 2023).

[9] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited September 11, 2023).

response plan if a breach occurs.[10] Immediate notification of a Data Breach is critical so that those impacted can take measures to protect themselves. Despite this guidance, PBI delayed the notification of the Data Breach.

The Current and Future Harms Caused by the Data Breach

41. Victims of data breaches are susceptible to becoming victims of identity theft.

42. Plaintiffs and Class Members face a lifetime of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs and the Class are incurring and will continue to incur such damage in addition to any fraudulent use of their PII.

43. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority," 17 C.F.R. § 248.201(9), and when "identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance.

44. PII is very valuable to criminals, as evidenced by the prices they will pay for it on the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information is sold at prices ranging from $40 to $200, and bank details have a price range of $50 to $200.[11]

45. Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[12]

---

[10] *Id*.

[11] *Your Personal Data Is for Sale on the Dark Web. Here's How Much It Costs,* DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on- the-dark-web-how-much-it-costs.

[12] *Here's How Much Your Personal Information Is Selling for on the Dark Web,* EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your- personal-

46. Social Security numbers are among the most sensitive kind of personal information and, when stolen, may be put to a variety of fraudulent uses. The Social Security Administration stresses that the loss of an individual's Social Security number, as occurred in the Data Breach here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[13]

47. Additionally, changing or canceling a stolen Social Security number is no easy task. An individual cannot obtain a new Social Security number without significant paperwork and evidence of misuse. An individual cannot prevent potential misuse of a Social Security number by simply changing their number. Instead, the individual must show evidence of actual, ongoing fraud to obtain a new Social Security number.

48. Even then, obtaining a new Social Security number may not work. According to the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[14]

49. Thus, consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is

---

information-is-selling-for-on-the-dark-web/.

[13] *Identity Theft and Your Social Security Number*, SOCIAL SECURITY ADMINISTRATION, https://www.ssa.gov/pubs/EN-05-10064.pdf.

[14] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015.), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s- hackers-has-millions-worrying-about-identity-theft.

considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[15]

50. The information compromised in the Data Breach is significantly more valuable than the loss of, for example, payment card information in a retailer data breach because, in that situation, victims can cancel or close payment card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—name, birthdate, and Social Security number.

51. This data commands a much higher price on the black market. "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[16]

52. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[17] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[18]

---

[15] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

[16] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x- price-of-stolen-credit-card-numbers.html.

[17] *See* SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentialsfetch- high-prices-in-the-online-black-market.

[18] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (Apr. 8, 2014), https://www.illuminweb.com/wp-

53. Identity thieves may use stolen data to commit bank fraud, credit card fraud, employer or tax-related fraud, government documents or benefits fraud, loan or lease fraud, phone or utilities fraud, among other forms of fraud.[19]

54. Criminals can use stolen PII to extort a financial payment by "leveraging details specific to a disease or terminal illness."[20] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion…By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[21]

55. Cybercriminals took the PII of Plaintiffs and Class Members to engage in identity theft and/or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activities resulting from the Data Breach may not come to light for years.

56. Theft of PII is serious. The Federal Trade Commission ("FTC") warns consumers that identity thieves use PII to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[22]

---

content/uploads/ill-mo-uploads/103/2418/health-systemscyber- intrusions.pdf.

[19] FTC Consumer Sentinel Network, Compare Identity Theft Report Types, https://public.tableau.com/app/profile/federal.trade.commission/viz/IdentityTheftReports/TheftTypesOverTime, (Last visited July 9, 2023).

[20] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcaredata- perfcon ("What Happens to Stolen Healthcare Data") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[21] *Id.*

[22] *See* Federal Trade Commission, *What to Know About Identity Theft*, FED. TRADE COMM'N CONSUMER INFO.

57. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose job opportunities or be denied loans for education, housing, or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

58. Identity theft, which costs Americans billions of dollars annually, occurs when an individual's PII is used without consent to commit fraud or other crimes. Victims of identity theft typically lose hundreds of hours dealing with the crime and hundreds, if not thousands, of dollars.

59. According to Javelin Strategy & Research, in 2018 alone, identity theft affected over 16.7 million individuals, causing a loss of over $16.8 billion.

60. Recent FTC data reveals that identify theft remains the top category of fraud reports received by the agency.[23] The FTC received over 1,100,000 reports of identity theft in 2022, and over 280,000 for the first quarter of 2023 alone.[24]

61. Identity thieves use personal information for various crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[25] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal

[23] FTC Consumer Sentinel Network, Federal Trade Commission, https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudandIDTheftMaps/AllReportsbyState, (Last visited July 9, 2023).
[24] *Id*.
[25] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

information is valuable to identity thieves, and if they can get access to it, they will use it" to, among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; or use the victim's information in the event of arrest or court action.[26]

62. With access to an individual's PII, criminals can do more than just empty a victim's bank account. They can also commit all manner of fraud, including (i) obtaining a driver's license or official identification card in the victim's name but with the thief's picture; (ii) using the victim's name and SSN to obtain government benefits; or (iii) filing a fraudulent tax return using the victim's information. In addition, identity thieves may even give the victim's personal information to police during an arrest.[27]

63. Consumers place a high value not only on their personal information but also on the privacy of that data. They do so because identity theft causes "significant negative financial impact on victims" in addition to severe distress and other strong emotional and physical reactions.

64. The United States Government Accountability Office ("GAO") explains that "[t]he term 'identity theft' is broad and encompasses many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit

[26] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN, https://www.experian.com/blogs/ask-experian/what-canidentity- thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/ (last accessed Mar. 21, 2022).

[27] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Mar. 21, 2023); *See* Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RES.

card account in someone else's name."[28] The GAO Report notes that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[29]

65. Further, as noted, there is the likelihood of a lapse in time between when the harm occurs to a victim of identity theft and when that harm is discovered, as well as a lapse between when the PII is stolen and when it is actually used. According to the GAO, which conducted a study regarding the growing number of data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[30]

66. A compromised or stolen Social Security number cannot be addressed as simply as, perhaps, a stolen credit card. An individual cannot obtain a new Social Security number without significant work. Preventive action to defend against the possibility of misuse of a Social Security number is not permitted; rather, an individual must show evidence of actual, ongoing fraud activity to obtain a new number. Even then, however, obtaining a new Social Security number may not suffice. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[31]

---

[28] *See* Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, U.S. Government Accountability Office Report to Congressional Requesters ("GAO Report") at 2 (June 2007), https://www.gao.gov/new.items/d07737.pdf, (Last visited July 10, 2023).
[29] *Id.*
[30] *See* GAO Report, at p.29.
[31] *Id.*

67. The PII compromised in the Data Breach demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained: "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[32]

68. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.[33]

69. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[34] Defendants did not rapidly or timely report to Plaintiffs and Class members that their PII had been stolen.

70. PBI offered victims twelve months of complimentary credit monitoring and identity restoration services through Kroll. The service offered by PBI is inadequate. Identity thieves often hold onto personal information in order to commit fraud years after such free programs expire.

71. As a result of the Data Breach, Plaintiffs and Class members' PII has been exposed to criminals for misuse. The injuries suffered by Plaintiffs and Class members, or likely to be suffered thereby as a direct result of Defendants' Data Breach, include:

a. unauthorized use of their PII;

---

[32] *Experts advise compliance not same as security*, RELIAS MEDIA (Mar. 1, 2015) https://www.reliasmedia.com/articles/134827-experts-advise-compliance-not-same-as-security (Last visited September 11, 2023).

[33] *2019 Internet Crime Report Released*, FBI, https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion. (Last visited September 11, 2023).

[34] *Id.*

b. theft of their personal and financial information;
c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;
d. damages arising from the inability to use their PII;
e. Improper disclosure of their PII;
f. loss of privacy, and embarrassment;
g. trespass and damage their personal property, including PII;
h. the imminent and certainly impending risk of having their confidential medical information used against them by spam callers and/or hackers targeting them with phishing schemes to defraud them;
i. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, and the stress, nuisance, and annoyance of dealing with all issues resulting from the Data Breach;
j. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class members' information on the Internet black market; and
k. damages to and diminution in value of their PII entrusted to Defendants.

72. In addition to a remedy for economic harm, Plaintiffs and Class members maintain an interest in ensuring that their PII is secure, remains secure, and is not subject to further misappropriation and theft.

73. Defendants disregarded the rights of Plaintiffs and Class members by (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that their network servers were protected against unauthorized intrusions; (ii) failing to disclose that Defendants did not have adequately robust security protocols and

training practices in place to adequately safeguard Plaintiffs' and Class members' PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; and (iv) failing to provide Plaintiffs and Class members prompt notice of the Data Breach.

74. The actual and adverse effects to Plaintiffs and Class members, including the imminent, immediate and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly and/or proximately caused by Defendants' wrongful actions and/or inaction and the resulting Data Breach require Plaintiffs and Class members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts, for which there is a financial and temporal cost. Plaintiffs and other Class members have suffered, and will continue to suffer, such damages for the foreseeable future.

CLASS ACTION ALLEGATIONS

75. Plaintiffs brings this action pursuant to Rule 23 of the Federal Rules of Civil Procedure, individually and on behalf of the following Nationwide Class:

> All persons in the United States whose PII was accessed, acquired, or compromised during the Data Breach as a result of the exploitation of PSC's MOVEit Application vulnerability (the "Class").

76. Specifically excluded from the Class are Defendants, their officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint venturers, or entities controlled by Defendants, and their heirs, successors, assigns, or other persons or entities related to or affiliated with Defendants and/or

their officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

77. Plaintiffs reserve the right to amend the Class definitions above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

78. This action may be certified as a class action under Federal Rule of Civil Procedure 23 because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

79. Numerosity (Rule 23(a)(1)): The Class is so numerous that joinder of all Class members is impracticable. Although the precise number of such persons is unknown, and the facts are presently within the sole knowledge of Defendants, Plaintiffs estimates that the Class is comprised of millions of Class members. The Class is sufficiently numerous to warrant certification.

80. Typicality of Claims (Rule 23(a)(3)): Plaintiffs' claims are typical of those of other Class members because they all had their PII compromised as a result of the Data Breach. Plaintiffs are members of the Class and her claims are typical of the claims of the members of the Class. The harm suffered by Plaintiffs are similar to that suffered by all other Class members that was caused by the same misconduct by Defendants.

81. Adequacy of Representation (Rule 23(a)(4)): Plaintiffs will fairly and adequately represent and protect the interests of the Class. Plaintiffs have no interest antagonistic to, nor in conflict with, the Class. Plaintiffs have retained competent counsel who are experienced in consumer and commercial class action litigation, including data breach class actions, and who will prosecute this action vigorously.

82. Superiority (Rule 23(b)(3)): A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class members is relatively small, the expense and burden of individual litigation make it impossible for individual Class members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendants will likely continue their wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for their wrongdoing as asserted herein.

83. Predominant Common Questions (Rule 23(a)(2)): The claims of all Class members present common questions of law or fact, which predominate over any questions affecting only individual Class members, including:

a. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
b. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
c. Whether Defendants' storage of Class Member's PII was done in a negligent manner;
d. Whether Defendants had a duty to protect and safeguard Plaintiffs' and Class members' PII;
e. Whether Defendants' conduct was negligent;
f. Whether Defendants' conduct violated Plaintiffs' and Class members' privacy;
g. Whether Defendants took sufficient steps to secure their customers' PII;
h. Whether Defendants were unjustly enriched;
i. The nature of relief, including damages and equitable relief, to which Plaintiffs and members of the Class are entitled.

84. Information concerning Defendants' policies is available from Defendants' records.

85. Plaintiffs know of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a class action.

86. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendants. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

87. Defendants have acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief and/or corresponding declaratory relief with respect to the Class as a whole.

88. Given that Defendants have not indicated any changes to their conduct or security measures, monetary damages are insufficient and there is no complete and adequate remedy at law.

CAUSES OF ACTION
COUNT I
NEGLIGENCE

89. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

90. Plaintiffs bring this claim individually and on behalf of the Class members.

91. Defendants knowingly collected, came into possession of, and maintained Plaintiffs' and Class members' PII, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

92. Defendants had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and Class members' PII.

93. Defendants had, and continue to have, a duty to timely disclose that Plaintiffs' and Class members' PII within their possession was compromised and precisely the type(s) of information that were compromised.

94. Defendants owed a duty of care to Plaintiffs and Class members to provide data security consistent with industry standards, applicable standards of care from statutory authority like Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected their customers' PII.

95. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and their customers. Defendants were in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

96. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential PII.

97. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII.

98. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to adequately and timely notify impacted consumers of the Data Breach; and

e. Failing to periodically ensure that their computer systems and networks had plans in place to maintain reasonable data security safeguards.

99. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiffs and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class members' PII within Defendant's possession.

100. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiffs' and Class members' PII.

101. Defendants, through their actions and/or omissions, unlawfully breached their duty to timely disclose to Plaintiffs and Class members that the PII within Defendant's possession might have been compromised and precisely the type of information compromised.

102. It was foreseeable that Defendants' failure to use reasonable measures to protect Plaintiffs' and Class members' PII would result in injury to Plaintiffs and Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

103. It was foreseeable that the failure to adequately safeguard Plaintiffs' and Class members' PII would result in injuries to Plaintiffs and Class members.

104. Defendants' breaches of duties owed to Plaintiffs and Class members caused Plaintiffs' and Class members' PII to be compromised.

105. But for Defendants' negligent conduct and breach of the above-described duties owed to Plaintiffs and Class members, their PII would not have been compromised.

106. As a result of Defendants' failure to timely notify Plaintiffs and Class members that their PII had been compromised, Plaintiffs and Class members were unable to take the necessary precautions to mitigate damages by preventing future fraud.

107. As a result of Defendants' negligence and breach of duties, Plaintiffs and Class members are in danger of imminent harm in that their PII, which is still in the possession of third parties, will be used for fraudulent purposes, and Plaintiffs and Class members have and will suffer damages including: a substantial increase in the likelihood of identity theft; the compromise, publication, and theft of their personal information; loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach; and overpayment for the services or products that were received without adequate data security.

COUNT II
Negligence *Per Se*

108. Plaintiffs re-allege and incorporate by reference herein all the allegations contained above.

109. Section 5 of the FTC Act, 15 U.S.C. 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendants of failing to use reasonable measures to protect Plaintiffs' and Class members' PII. Various FTC publications and orders also form the basis of Defendants' duty.

110. Defendants violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Plaintiffs' and Class members' PII and not complying with industry standards.

111. Defendants' conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach.

112. Defendants' violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

113. Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

114. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and Class members.

115. As a result of Defendants' negligence, Plaintiffs and the other Class members have been harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

COUNT III
BREACH OF IMPLIED CONTRACT

116. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

117. Plaintiffs and the Class provided and entrusted their PII to Defendants. Plaintiffs and the Class provided their PII to Defendants as part of Defendants' regular business practices.

118. Defendants should have been aware that they had a minimum duty to alert Plaintiffs and Class embers that their data was compromised "without unreasonable delay."

119. Thus, when Defendants took Plaintiffs' and Class members' PII, it entered into implied contracts with Plaintiffs and Class members by which Defendants agreed to safeguard and protect such information and to keep such information secure and confidential. Implied in these exchanges was a promise by Defendants to ensure that the PII of Plaintiffs and Class members in its possession was secure.

120. Pursuant to these implied contracts, Plaintiffs and Class members provided Defendants with their PII in order for Defendants to provide their services, for which Defendants are compensated. In exchange, Plaintiffs understood, and Defendants agreed, among other things, that Defendants would: (1) provide services to Plaintiffs and Class

members; (2) take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' PII; (3) protect Plaintiffs' and Class members PII in compliance with federal and state laws and regulations and industry standards; and (4) notify Plaintiffs and Class members in compliance with state laws and regulations.

121. Implied in these exchanges was a promise by Defendants to take adequate measures to protect Plaintiffs' and Class members' PII, and notify Plaintiffs and Class members where data safeguards failed.

122. A material term of this contract is a covenant by Defendants that they would take reasonable efforts to adequately secure that information. Defendants breached this covenant by allowing Plaintiffs' and Class members' PII to be accessed in the Data Breach.

123. Indeed, implicit in the agreement between Defendants and their customers was the obligation that both parties would maintain information securely and respond accordingly if that information was compromised.

124. These exchanges constituted an agreement and meeting of the minds between the parties: Plaintiffs and Class members would provide their PII in exchange for services by Defendants. These agreements were made by Plaintiffs and Class members as Defendants' customers.

125. When the parties entered into an agreement, mutual assent occurred. Plaintiffs and Class members would not have disclosed their PII to Defendants but for the prospect of utilizing Defendants' services. Conversely, Defendants presumably would not have obtained Plaintiffs' and Class members' PII if they did not intend to provide Plaintiffs and Class members with their services.

126. Defendants were therefore required to reasonably safeguard and protect the PII of Plaintiffs and Class members from unauthorized disclosure and/or use and, as promptly as reasonable, notify Plaintiffs and Class members when it failed in that duty.

127. Plaintiffs and Class members accepted Defendants' offer of services and fully performed their obligations under the implied contract with Defendants by providing their PII, directly or indirectly, to Defendants, among other obligations.

128. Plaintiffs and Class members would not have entrusted their PII to Defendants in the absence of their implied contracts with Defendants and would have instead retained the opportunity to control their PII.

129. Defendants breached the implied contracts with Plaintiffs and Class members by failing to reasonably safeguard and protect Plaintiffs' and Class members' PII.

130. Defendants' failure to implement adequate measures to protect the PII of Plaintiffs and Class members violated the purpose of the agreement between the parties.

131. Defendants further failed to adequately and promptly notify Plaintiffs and Class members that their PII had been compromised.

132. Instead of spending adequate financial resources to safeguard Plaintiffs' and Class members' PII, which Plaintiffs and Class members were required to provide to Defendants, Defendants instead used that money for other purposes, thereby breaching their implied contracts with Plaintiffs and Class members.

133. As a proximate and direct result of Defendants' breaches of their implied contracts with Plaintiffs and Class members, Plaintiffs and the Class members suffered damages as described in detail above.

COUNT IV
BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING

134. Plaintiffs reallege and reincorporate every allegation set forth in the preceding paragraphs as though fully set forth herein.

135. Every contract has an implied covenant of good faith and fair dealing between the parties to it, which is an independent duty requiring every party in a contract to implement the agreement as intended, without using means to undercut the purpose of the transaction. This duty may be breached even when there is no breach of a contract's actual and/or express terms.

136. Plaintiffs and Class Members have complied with and performed all conditions of their contracts with Defendants.

137. Defendants breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII and failing to timely and accurately disclose the Data Breach to Plaintiffs and Class Members.

138. Defendants acted in bad faith in denying Plaintiffs and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them compensable injury in an amount to be determined at trial.

COUNT V
BREACH OF FIDUCIARY DUTY

139. Plaintiffs reallege and reincorporate all previous paragraphs as if fully set forth below.

140. As a condition of obtaining services from Defendants, Plaintiffs and Class Members gave Defendants their PII in confidence, believing that Defendants would protect

that information. Plaintiffs and Class members would not have provided Defendants with this information had they known it would not be adequately protected. Defendants' acceptance and storage of Plaintiffs' and Class members' PII created a fiduciary relationship between Defendants and Plaintiffs and Class Members. In light of this relationship, Defendants were and are required to act primarily for the benefit of their customers, which includes safeguarding and protecting Plaintiffs' and Class members' PII.

141. Defendants had and continue to have a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship. Defendants breached that duty by failing to properly protect the integrity of the systems containing Plaintiffs' and Class members' PII, failing to comply with minimum data security practices, and otherwise failing to safeguard Plaintiffs' and Class members' PII that they collected.

142. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach; and/or (vii) overpayment for the services that were received without adequate data security.

COUNT VI
UNJUST ENRICHMENT

143. Plaintiffs incorporate the above allegations as if fully set forth herein.

144. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

145. Plaintiffs conferred a benefit upon Defendants by using Defendants' services.

146. Defendants appreciated or had knowledge of the benefits conferred upon themselves by Plaintiffs and Class members. Defendants also benefited from the receipt of Plaintiffs' PII as this was used for Defendants to administer their services to Plaintiffs and the Class.

147. Under principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiffs' services because Defendants failed to adequately protect their PII. Plaintiffs and the proposed Class would not have provided their PII to Defendants or utilized their services had they known Defendants would not adequately protect their PII.

148. Defendants should be compelled to disgorge into a common fund for the benefit of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT VII
DECLARATORY JUDGMENT

149. Plaintiffs reallege and reincorporate every allegation set forth in the preceding paragraphs as though fully set forth herein.

150. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

151. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' PII and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII. Plaintiffs allege that Defendants' data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury due to the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future.

152. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owe a legal duty to secure consumers' PII and to timely notify consumers of a data breach under the common law and Section 5 of the FTC Act;
b. Defendants have breached their duty to Plaintiffs and the Class by allowing the Data Breach to occur;
c. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure consumers' PII. This Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry standards to protect consumers' PII; and
d. Defendants' ongoing breaches of said duty continue to cause harm to Plaintiffs and the Class.

153. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach with Defendants. The risk of another such breach is real, immediate, and substantial. If Defendants allow another data breach, Plaintiffs and Class Members will not have an

adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

154. Plaintiffs and the Class, therefore, seek a declaration that (1) each of Defendants' existing security measures do not comply with their obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect consumers' PII, and (2) to comply with their duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;
b. Engaging third-party security auditors and internal personnel to run automated security monitoring;
c. Auditing, testing, and training their security personnel regarding any new or modified procedures;
d. Segmenting user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;
e. Conducting regular database scanning and security checks;
f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
g. Purchasing credit monitoring services for Plaintiffs and Class Members for their respective lifetimes; and
h. Meaningfully educating Plaintiffs and Class Members about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

155. The Court should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with the law and industry standards to protect Plaintiffs and Class Members' PII.

156. The hardship to Plaintiffs and Class Members if an injunction were not issued exceeds the hardship to Defendants if an injunction were issued. Plaintiffs and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

157. Issuance of the requested injunction would not disserve the public interest. On the contrary, such an injunction would benefit the public by preventing another data breach of Defendants' systems, thus eliminating the additional injuries that would result to Plaintiffs and Class Members whose PII would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seek judgment against Defendants, as follows:

(a) For an order determining that this action is properly brought as a class action and certifying Plaintiffs as the representatives of the Class and their counsel as Class Counsel;

(b) For an order declaring the Defendants' conduct violates the laws referenced herein;

(c) For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;

(d) For damages in amounts to be determined by the Court and/or jury;

(e) An award of statutory damages or penalties to the extent available;

(f) For pre-judgment interest on all amounts awarded;

(g) For an order of restitution and all other forms of monetary relief;

(h) For declaratory and/or injunctive relief, as set forth herein; and

(i) Such other and further relief as the Court deems necessary and appropriate.

DEMAND FOR TRIAL BY JURY

Plaintiffs demands a trial by jury of all issues so triable.

Dated: September 18, 2023

SHAPIRO HABER & URMY LLP

/s/ Edward F. Haber
Edward F. Haber (BBO# 215620)
Ian J. McLoughlin (BBO# 647203)
Shapiro Haber & Urmy LLP
One Boston Place, Suite 2600
Boston, MA 02108
Tel: (617) 439-3939
Fax: (617) 439-0134
ehaber@shulaw.com
imcloughlin@shulaw.com

Robert C. Schubert
Amber L. Schubert
Schubert Jonckheer & Kolbe LLP
2001 Union Street, Suite 200
San Francisco, California 94123
Tel: (415) 788-4220
Fax: (415) 788-0161
rschubert@sjk.law
aschubert@sjk.law

Counsel for Plaintiffs and the Putative Class

Exhibit A

pbi

July 14, 2023

Megan C. Schwarz
1295 5th Ave. Apt. 13D
New York, NY 10029-3131

P14T497

Dear Megan C. Schwarz:

Pension Benefit Information, LLC ("PBI") provides audit and address research services for insurance companies, pension funds, and other organizations, including Teachers Insurance and Annuity Association of America (TIAA). PBI is providing notice of a third-party software event that may affect the security of some of your information. Although we have no indication of identity theft or fraud in relation to this event, we are providing you with information about the event, our response, and additional measures you can take to help protect your information, should you feel it appropriate to do so.

What Happened? On or around May 31, 2023, Progress Software, the provider of MOVEit Transfer software disclosed a vulnerability in their software that had been exploited by an unauthorized third party. PBI utilizes MOVEit in the regular course of our business operations to securely transfer files. PBI promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on our systems. Through the investigation, we learned that the third party accessed one of our MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded data. We then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. We recently completed this review.

What Information Was Involved? Our investigation determined that the following types of information related to you were present in the server at the time of the event: name, Social Security number, gender, date of birth, and address.

What We Are Doing. We take this event and the security of information in our care seriously. Upon learning about this vulnerability, we promptly took steps to patch servers, investigate, assess the security of our systems, and notify potentially affected customers and individuals associated with those customers. In response to this event, we are also reviewing and enhancing our information security policies and procedures.

While we are unaware of any identity theft or fraud as a result of this event, as an additional precaution, PBI is offering you access to 24 months of complimentary identity monitoring services through Kroll. Details of this offer and instructions on how to activate these services are enclosed with this letter.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please also review the enclosed *Steps You Can Take to Help Protect Personal Information*, which contains information on what you can do to safeguard against possible misuse of your information. You can also activate the identity monitoring services that we are offering.

For More Information. If you have additional questions, you may call our toll-free assistance line at (866) 373-7560 Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern time (excluding U.S. holidays). You may also write to PBI at 333 South Seventh Street, Suite 2400, Minneapolis, MN 55402.

Sincerely,

John Bikus
President
Pension Benefit Information, LLC

Steps You Can Take To Help Protect Personal Information

Activate Your Monitoring Services

To help relieve concerns and restore confidence following this event, we have secured the services of Kroll to provide identity monitoring at no cost to you for 24 months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.[1]

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.
*You have until **October 4, 2023** to activate your identity monitoring services.*
Membership Number: **DYVJ73399-P**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional Information

- **Single Bureau Credit Monitoring**. You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.
- **Fraud Consultation**. You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.
- **Identity Theft Restoration**. If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

- Full name (including middle initial as well as Jr., Sr., II, III, etc.);
- Social Security number;
- Date of birth;
- Addresses for the prior two to five years;
- Proof of current address, such as a current utility bill or telephone bill;
- A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
- A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state attorney general. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Kentucky residents, the Kentucky Attorney General – Office of Consumer Protection may be contacted at: 1024 Capital Center Drive, Suite 200, Frankfort, Kentucky 40601; 1-800-804-7556; and https://www.ag.ky.gov/Resources/Consumer-Resources/Consumers/Pages/Identity-Theft.aspx.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For Massachusetts residents, you have the right to obtain any police report filed in regard to this event. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event.